MINUTES
Strategic Planning Committee

DATE	September 4, 2002
TIME	10:00 AM
LOCATION	Kinkead Building, 6th Floor Conference Room Carson City
RECORDER	Alisanne Maffei, Strategic Planner

ATTENDEES

Name	Attend ✓	Name	Attend ✓
Chair – Mike Hillerby, Governor's Office	✓	Co-Chair – Mark Blomstrom, DoIT	✓
Chuck Chinnock, Taxation		Terry Savage, DoIT	✓
Chuck Conner, DMV	✓	Scott Sisco, Cultural Affairs	✓
Kathy Shabi, DETR	✓	Freeman Johnson, CNR	✓
Sara Jones, Cultural Affairs	✓	P. Forrest Thorne, PEBS	✓
Alisanne Maffei, DoIT	✓	Doug Walther, B&I	✓
Dorothy Martin, DoIT	✓	Ginny Lewis, DMV	
Dana Mathiesen, DMV		Dan Goggiano, DoIT	✓
Kathy Ryan, DoIT	✓	Tom Stephens, NDOT	
Pam V. Sutton, DoIT	✓		

CALL TO ORDER

I Introduction

- Mike Hillerby opened the meeting.
- Mike Hillerby announced Mark Blomstrom was going to head up the IT Technical Standards and Architecture Committee. Alisanne Maffei will now be the Co-chair of the IT Strategic Planning Committee.

II Review and Approval of the Minutes

- After review of the June meeting minutes, it was motioned and seconded to accept the minutes. There were no other comments. The minutes from June 19, 2002, were accepted as presented.

III DISCUSSION

- Terry Savage provided an update on the Information Technology Advisory Board (ITAB) meeting. Descriptions of presentations to ITAB included mainframe requirements, security initiative, preliminary rates, and Top Ten IT Issues. The opportunity to cover high visibility issues with the legislators was discussed.
- The Committee heard presentations on the following areas: feedback discussion on e-gov committee Strategic Plan with Pam Sutton, update on security committee/implementation of security PSP's and budget impact by Donna Crutcher, and presentation of the sysplex /mainframe upgrade by Dorothy Martin.

e-gov Strategic Plan:

Pam Sutton explained a technical plan will be developed in conjunction with the e-gov strategic plan as the next step. Sara Jones had provided detailed feedback on the plan. Alisanne Maffei has arranged for META Research Group to provide a complimentary review of the plan. Sara indicated the State Data Center Librarian is available for research support.

Security Initiatives:

Terry Savage provided an update on the security initiatives. Work is being done with the Budget Division to figure out how to fund the initiatives and with minimal impact to the smaller agencies. Consultant Ed Perry is trying to determine how to protect federal funding as well as reduce the impact to agencies. The federal government pays 70 to 80% of the total State budgets, resulting in federal support for IT security.

Mark Blomstrom explained that is was getting easy for “hackers” to execute automatic attacks into networks by hunting for the weakest points. He stated that it will continue to increase as a risk with Nevada trying to avoid getting a big hit. The security expenditures to provide the necessary deterrence are like automobile insurance against the probabilities to get hit or not. Terry Savage stated some of the risks must be quantified, identifying the high risks. Sara Jones said we should look at the rates as the deductible you pay for insurance. Also for consideration, the Library has a vault for the high risk items to reduce overall risks.

Scott Sisco made the case for the small agencies stating their issues. It is tough to take from the limited funds available to apply something to the security initiatives. Sara Jones reiterated the need for impact analysis on implementing security PSP’s. Even with approval of new IT security positions, there will be an impact to the agency staff. Sara doesn’t have disagreement with the standards; however at issue is now can the NSLA and other smaller agencies handle the costs to pay for them. The standards must be prioritized. Terry agreed the standards are to be prioritized since all the funding won’t be received. Woody Thorne stated that the Security Committee needs to take a risk management approach.

Mainframe Upgrade

Dorothy Martin and Dan Goggiano presented "State of Nevada Sysplex today, Tomorrow and Beyond". Today's current situations including the hardware issues were discussed. IBM is concluding its support for the R35 (165 mips) and peak time utilization is exceeding 70% and increasing as well as the R46 (447 mips) reaching saturation. The Enterprise Server utilization and impact of utilization exceeding 90% was presented. There are 43 customers; eight major customers with one using 55% of the services. Assumptions, process, options and impact to the State for the upgrade were provided. The analysis covered: z900 series replacement, R35 upgrade, or no upgrade/business as usual. The recommendation was made for the z900 hardware architecture replacement based on the long term support horizon, the increased capacity, capacity on demand and memory on demand capabilities.

- The Committee also discussed IT assessments, imaging issues and employee IT breaches:

Federal cost recovery must be what agencies are charged in proportion to the benefits received from the services. Security cannot be charged for on an hourly basis. DoIT is working with the Budget Office and Governor to determine how to handle any changes and proceed forward.

Mark Blomstrom discussed the imaging laws and the need for strategic direction. Needs are to be identified to be able to plan accordingly. The enterprise wide planning for records retention schedules and overall architecture needs to be addressed. It was decided to table further discussion to another agenda for an in-depth discussion. Scott Sisco and Sara Jones reiterated that the question needs to be asked why something needs to be stored, not to just buy storage without the proper evaluation.

Specific examples of Employee Breeches were disclosed by Alisanne Maffei (i.e.: installation/use of unauthorized software, use of computing resources for illegal activities, and use of computing resources for personal profit).

Cyber Attacks Composition:	Percent (Total = 100%)
Authorized Internal Employees	53%
Unauthorized Internal Employees	20%
Former Employees	12%
Competitors/Hackers/Crackers	15%

Source: Gartner State of Nevada IT Strategic Planning Committee Teleconference, 6/19/02 Note: Other sources place Authorized Internal Employee breaches 57% - 71%

Major Direct Insider Threats:
Bribery: Employee offered cash for proprietary or confidential data
Social Engineering: Employee manipulated to divulge information e.g.: logon
Group Collusion: Employees share collective knowledge for access to information

Source: 2000 Computer Crime Report by FBI/Computer Security Institute

Top Three Security Breaches performed by Employees:
Installation/Use of Unauthorized Software
Use of Computing Resources for Illegal Activities
Use of Computing Resources for Personal Profit

A Possible Disgruntled Employee Scenario: Logon by using another employee's authentication information to remain undetected, perhaps by requesting logon info from IT help desk or the sharing of passwords; or possible data wire tap or backup tape theft to obtain information. Then the employee abuses processes and circumvents control measures to make money or cause damage.

Remember: percentages are higher due to unreported or undetected attacks.

IV WRAP UP

The next meeting of the IT Strategic Planning Committee will be targeted for December, 2002.

ACTION ITEMS

Item No.	Description	Assigned To
1.	Create a proposal to draft a pilot program and research into lease agreement providing IT hardware, software, and periodic replacement on a statewide basis for submittal to the Legislature.	Mark Blomstrom, Alisanne Maffei
2.	Report on examples of Employee Breeches	Alisanne Maffei
3.	Discuss Economic Task Force recommendations and impact	All